

Patent  
Attorney's Docket No. 032326-192

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	
Jean-Sébastien CORON et al	)	Group Art Unit: Unassigned
Application No.: Unassigned	)	Examiner: Unassigned
Filed: January 30, 2002	)	
For: SIGNATURE SCHEMES BASED ON	)	
DISCRETE LOGARITHM WITH	)	
PARTIAL OR TOTAL MESSAGE	)	
RECOVERY	)	

**INFORMATION DISCLOSURE STATEMENT  
TRANSMITTAL LETTER**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

Enclosed is an Information Disclosure Statement and accompanying form PTO-1449 for the above-identified patent application.


- ☒ No additional fee for submission of an IDS is required.
- ☐ The fee of \$180.00 (126) as set forth in 37 C.F.R. § 1.17(p) is also enclosed.
- ☐ A certification under 37 C.F.R. § 1.97(e) is also enclosed.
- ☐ A certification under 37 C.F.R. § 1.97(e), and the fee of \$180.00 (126) as set forth in 37 C.F.R. § 1.17(p) are also enclosed.
- ☐ Charge \$\_\_\_\_\_ to Deposit Account No. 02-4800 for the fee due.
- ☐ A check in the amount of \$\_\_\_\_\_ is enclosed for the fee due.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800. This paper is submitted in duplicate.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

By:   
James A. LaBarre  
Registration No. 28,632

Date: January 30, 2002

Patent  
Attorney's Docket No. 032326-192

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	
	)	
Jean-Sébastien CORON et al	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: January 30, 2002	)	
	)	
For: SIGNATURE SCHEMES BASED ON	)	
DISCRETE LOGARITHM WITH	)	
PARTIAL OR TOTAL MESSAGE	)	
RECOVERY	)	

**INFORMATION DISCLOSURE STATEMENT**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. §1.56, Applicants hereby submit the following information in conformance with 37 C.F.R. §§ 1.97 and 1.98. A copy of each document cited below is enclosed.

**Foreign Patent Applications**

<b>Publication No.</b>	<b>Country</b>	<b>Publication Date</b>
0639907A1	Europe	02/22/1995

**Other Documents**

Nyberg, Kaisa, *"Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem"*, Kluwer Academic Publishers, Netherlands, January 1996, Vol. 7, No. 1-2, pps. 61-81.

Nyberg, Kaisa et al, *"A new Signature Scheme Based on the DSA Giving Message Recovery"*, Proceedings of the 1<sup>st</sup> ACEM Conference on Computer and Communications Security, 3-5 May 1993, pps. 58-61.

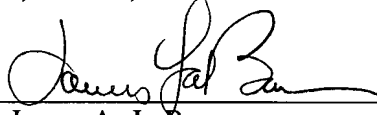
Information Disclosure Statement  
Application No. Unassigned  
Attorney's Docket No. 032326-192  
Page 2

These references were cited in an International Search Report for the corresponding PCT application. A copy of that Search Report is also being submitted herewith.

To assist the Examiner, the reference is listed on the attached form PTO-1449. It is respectfully requested that an initialled copy of this form be returned to the undersigned.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By:   
James A. LaBarre  
Registration No. 28,632

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

Date: January 30, 2002

Substitute for form 1449A/PTO  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	ATTORNEY'S DKT No. <b>032326-192</b>	APPLICATION No. Unassigned
	APPLICANT <b>Jean-Sébastien CORON et al</b>	
	FILING DATE	GROUP Unassigned

[illegible][illegible]

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Include name of author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.		
	Nyberg, Kaisa, <i>"Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem"</i> , Kluwer Academic Publishers, Netherlands, January 1996, Vol. 7, No. 1-2, pps. 61-81.		
	Nyberg, Kaisa et al, <i>"A new Signature Scheme Based on the DSA Giving Message Recovery"</i> , Proceedings of the 1 <sup>st</sup> ACEM Conference on Computer and Communications Security, 3-5 May 1993, pps. 58-61.		
Examiner Signature		Date Considered	